UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA

BENJAMIN FONTENOT, ***individually and on behalf of all others similarly situated*****,**

Case No.:_____

Plaintiff,

v.

DEMAND FOR A JURY TRIAL

ACADIAN AMBULANCE SERVICE, INC.

Defendant.

CLASS ACTION COMPLAINT

Plaintiff Benjamin Fontenot ("Plaintiff") brings this Class Action Complaint against Defendant Acadian Ambulance Service, Inc. ("Acadian" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges as follows:

INTRODUCTION

1. Acadian, a private ambulance service business based in Lafayette, Louisiana, operates throughout Louisiana, Texas, Tennessee, and Mississippi. Defendant failed to implement and maintain reasonable data security measures. As a result, in June 2024, a well-known cybercriminal organization called Daixin Team accessed and exfiltrated Plaintiff's and Class Members' personally identifiable information (PII) and protected health information (PHI), including full names, Social Security numbers, dates of birth, medical record numbers, and medical and treatment information (the "Data Breach")

2. Daixin Team demanded that Defendant pay a ransom of $7,000,000 for the return of PII stolen in the Data Breach. Defendant refused to pay this ransom, instead offering to pay $173,000, which Daixin Team rejected.[1] As a result, Plaintiff's, and Class Members' PII and PHI

[1] *Id*.

is at continued risk of being leaked on the dark web.

3. Despite the now certain fact that PII and PHI stolen in the Data Breach will be used maliciously, Defendant did not start notifying victims of the Data Breach, including Plaintiff, until July—long after recognizing the risk that Plaintiff and Class Members were facing.

4. Although Defendant has reprehensibly chosen to keep many details of the Data Breach secret, the evidence available thus far indicates that it is more likely than not that Defendant failed to implement and maintain reasonable data security measures. For example, Defendant did not properly encrypt or redact PII and PHI, retained PII and PHI longer than necessary, and failed to adequately secure user credentials for internet-facing applications on its network.

PARTIES

Plaintiff Benjamin Fontenot

5. Plaintiff Benjamin Fontenot is a resident and citizen of Saint Landry, Louisiana, where he intends to remain. Plaintiff was employed by Defendant from 2004-2018 and again from 2020-2022.

Defendant Acadian Ambulance Service

6. Defendant is a private ambulance service business incorporated in the State of Louisiana and headquartered at 130 E. Kaliste Saloom Road, Lafayette, LA 70508.

JURISDICTION AND VENUE

7. This Court has original subject-matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d). First, because the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs. Second, because this class action involves a putative class of over 100 members. And third, because there is sufficient diversity—while Defendant's principal place of business is in Louisiana, many Class Members are citizens of different states.

8. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business is in Louisiana, and Defendant regularly conducts business in Louisiana, and has a location in New Orleans, Louisiana.

9. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, Defendant conducts substantial business in this District, and Defendant is headquartered in Lafayette, Louisiana.

FACTUAL ALLEGATIONS

Background

10. Plaintiff and the Class Members, as current or former employees and customers, reasonably relied (directly or indirectly) on this large business to keep their sensitive PII and PHI confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII and PHI. People demand security to safeguard their PII PHI, especially when Social Security numbers and sensitive health information are involved as here.

11. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII and PHI from involuntary disclosure to third parties and as evidenced by the Data Breach, it failed to adhere to that duty.

The Data Breach

12. On or around June 2024, Daixin Team executed a foreseeable attack of Defendant's computer network that allowed it to steal the highly sensitive PII and PHI of

approximately 11 million customers and employees.[2]

13. Recent articles covering the breach have stated that impacted PII included full names and Social Security numbers, dates of birth, medical record numbers, and medical treatment information.[3]

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

14. It is well known that PII and PHI, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

15. At the time of the Data Breach, the specific threat posed by Daixin Team was known, or should have been known, by Defendant. Experts have described Daixin Team as "a cybercrime group that is actively targeting U.S. businesses, predominantly in the Healthcare and Public Health (HPH) Sector, with ransomware and data extortion operations.[4]

16. At the time, Daixin Team has committed other such well documented techniques to target providers like Defendant. As one publication noted in a report about the Data Breach, "Daixin Team cybercrime actors have caused ransomware incidents at multiple HPH Sector organizations[.]"[5]

17. On October 21, 2022, the FBI and CISA released a joint advisory (the "Joint Advisory") detailing the risk posed by Daixin Team to Healthcare and Public Health Sector providers, the common techniques employed by Daixin Team, and mitigation measures known to prevent Daixin Team attacks.[6]

---

[2] https://www.cpomagazine.com/cyber-security/acadian-ambulance-services-leaks-protected-health-information-after-cyber-attack/ (last accessed August 1, 2024).
[3] *Id*.
[4] https://www.cisa.gov/sites/default/files/2023-07/aa22-294a-stopransomware-daixin-team.pdf (last accessed August 1, 2024).
[5] *Id.*
[6] *See Id*.

Defendant Failed to Implement & Maintain Reasonable Security

18. As discussed above, the Joint Advisory details the specific methods of attack used by Daixin Team, along with how to prevent them.

19. Specifically, "Daixin actors gain initial access to victims through virtual private network (VPN) services."[7]

20. Given that Daixin Team likely effectuated the Data Breach through compromised computer systems, it is more likely than not that the "bad practices" identified by CISA were employed by Defendant at the time of the Data Breach.

21. The access to and exfiltration of PII and PHI by Daixin Team would not have occurred but for Defendant's failure to implement and maintain the data security measures discussed in the Joint Advisory and other advisory materials.

22. Regardless of Defendant's failure to properly secure and monitor PII and PHI, Defendant was also grossly negligent in its decision to not properly encrypt or redact the PII and PHI in its possession, as well as its decision to hold PII and PHI for longer than it had a legitimate use. For example, Plaintiff has not been affiliated with Defendant for two years. Yet, Defendant inexplicably decided to continue storing Plaintiff's and other Class Members' PII on its systems long after their affiliation with Defendant ended.

23. Several best practices have been identified for entities that store PII and PHI, like Defendant, including but not limited to educating all employees; using strong passwords; implementing multi-layer security measures such as firewalls, anti-virus, and anti-malware software; encrypting data to make it unreadable without a key; employing multi-factor authentication; backing up data; and limiting employee access to sensitive information.

[7] *Id*.

24. Other best cybersecurity practices that are standard in the data security industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

25. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

26. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

27. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because Defendant failed to properly maintain and safeguard their computer systems and network. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect PII and PHI;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to ensure that their vendors with access to their computer systems and data

employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PII and PHI it created, received, maintained, and/or transmitted;

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII and PHI to allow access only to those persons or software programs that have been granted access rights;

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII and PHI;

j. Failing to train all members of their workforces effectively on the policies and procedures regarding PII and PHI;

k. Failing to render the electronic PII and PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals;

l. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

m. Failing to adhere to industry standards for cybersecurity as discussed above; and,

n. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII and PHI.

28. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII and PHI by allowing cyberthieves to access Defendant's online insurance

application flow, which provided unauthorized actors with unsecured and unencrypted PII and PHI.

29. Consequently, as detailed below, Plaintiff and Class Members now face an immediate, heightened risk of fraud and identity theft. Additionally, Plaintiff and the Class Members lost the benefit of the bargain they made with Defendant.

The Theft of PII and PHI Has Severe & Long-Lasting Consequences

30. The ramifications of Defendant's failure to keep Plaintiff's and Class Members' PII and PHI secure are long lasting and severe. Once PII and PHI are stolen, particularly Social Security numbers as here, fraudulent use of that information and damage to victims is likely to continue for years.

31. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[8]

32. This is because any victim of a data breach is exposed to severe consequences regardless of the nature of the data. In fact, criminals steal personally identifiable information to monetize it by selling the stolen data on the black market to identity thieves who aim to extort and harass victims or take over their identities to engage in illegal financial transactions under the victims' names.

33. Social Security numbers are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers

[8] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited May 26, 2023).

are taken and used by hackers. Even if they know their Social Security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

34. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

35. By failing to properly notify Plaintiff and the Class Members of the Data Breach, Defendant exacerbated their injuries. Specifically, by depriving them of the chance to take speedy measures to protect themselves and mitigate harm, Defendant allowed their injuries to fester and the damage to spread.

36. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding

> payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[9]

37. In addition to opening new bank or payment card accounts, attackers can use an individual's Social Security number, in combination with information like names, addresses, dates of birth, and/or phone numbers, to bypass account security protocols and access an individual's existing bank and payment card accounts.[10]

38. Trying to change or cancel a stolen Social Security number is incredibly difficult, if not impossible. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

39. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[11]

40. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their

---

[9] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed May 26, 2023).

[10] *See* https://reasonlabs.com/blog/7-things-hackers-can-do-with-your-stolen-social-security-number-and-6-ways-to-protect-it (last visited May 26, 2023); https://www.moneytalksnews.com/slideshows/heres-what-hackers-can-do-with-your-social-security-number/ (last visited May 26, 2023).

[11] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited May 26, 2023).

birthdate, birthplace, and mother's maiden name.[12]

41. It can take years for victims to notice their identity was stolen—giving criminals plenty of time to sell one's personal information to the highest bidder.

42. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

43. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

44. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[13]

---

[12] *See* https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2007/m07-16.pdf (last visited May 26, 2023).

[13] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records*

45. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

46. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

47. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

48. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

49. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[14] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social

---

for Sale in Underground Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance- finn/ (last visited on May 26, 2023).

[14] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 26, 2023).

Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[15] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

50. As demonstrated by the repeated attempts at identity theft and fraud that Plaintiff has suffered, that is exactly what is happening to Plaintiff and Class Members. And it is reasonable for any trier of fact, including this Court or a jury, to find that the stolen PII and PHI (of Plaintiff and the other Class Members) is being misused—and that such misuse is fairly traceable to Defendant's data breach.

51. Responsible for handling highly sensitive personal information, Defendant knew or should have known the importance of safeguarding PII and PHI. Defendant also knew or should have known of the foreseeable consequences of a data breach. These consequences include the significant costs imposed on victims of the breach. Still, Defendant failed to take adequate measures to prevent the data breach.

52. Due to Defendant's inadequate practices, the PII and PHI of Plaintiff and Class Members were exposed to criminals. In other words, Defendant disclosed and exposed its PII and PHI to malicious operators and criminals. These criminals engage in disruptive and unlawful activities such as online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud)—all using stolen PII.

53. Given the nature of Defendant's Data Breach it is foreseeable that the compromised

[15] *Id* at 4.

PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, simple credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[16] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

55. To date, Defendant has not offered Plaintiff and Class Members *any* sort of recovery or protective service in response to the Data Breach. This is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly considering the PII at issue here.

56. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures to protect PII and PHI that it maintained.

The Value of PII

57. Stolen personal information is one of the most valuable commodities on the information black market. According to Experian, a credit-monitoring service, stolen personal information can sell for over $1,000.00 (depending on the type of information).[17]

---

[16] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed May 26, 2023).

[17] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 26, 2023).

58. The value of Plaintiff's and Class Members' personal information on the black market is considerable. Stolen personal information trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites. Thus, after charging a substantial fee, criminals make such stolen information publicly available.

59. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[18] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[19]

60. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is likely readily available to others, and the rarity of the PII has been destroyed, thereby causing additional loss of value.

61. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[20]

Defendant Failed to Comply with FTC Guidelines

[18] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited May 26, 2023).
[19] *See* https://datacoup.com/ (last visited May 26, 2023).
[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited May 26, 2023).

62. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[21]

63. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[22] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[23]

64. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[24] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

---

[21] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited May 26, 2023)

[22] 17 C.F.R. § 248.201 (2013).

[23] *Id*.

[24] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed May 26, 2023).

65. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[25]

66. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the

[25] FTC, *Start with Security*, *supra* note 59.

network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

67. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

68. Since Class Members entrusted Defendant with their PII, either directly or indirectly, Defendant had, and continues to have, a duty to keep their PII secure.

69. Plaintiff and the other Class Members reasonably expected that when they provide PII to Defendant that such PII would be protected and safeguarded.

70. Defendant was at all times fully aware of its obligation to protect the personal data of its customers and current and former employees, including Plaintiff and Class Members. Defendant was also aware of the significant repercussions if it failed to do so.

71. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data—including Plaintiff's and Class Members' full names, Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury as A Result of Defendant's Inadequate Security and The Data Breach It Allowed.

72. Plaintiff and Class Members reasonably expected Defendant to provide adequate security protections for their PII and PHI, and therefore, entrusted Defendant with sensitive personal information, including their Social Security numbers.

73. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to work for Defendant or utilize Defendant's services as a customer, Plaintiff and other Class Members reasonably understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

74. Cybercriminals target and capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff have also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

75. The cybercriminals who targeted and obtained Plaintiff's and Class Members' PII

and PHI may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

76. Additionally, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, which can impair their ability to gain employment or obtain a loan.

77. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

78. Furthermore, certain PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[26]

79. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and Class Members at an imminent, immediate, and continuing

[26] *Id.*

increased risk of identity theft and identity fraud.[27] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[28] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[29] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

80. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages and will continue to suffer damages.

Plaintiff Benjamin Fontenot's Experience

81. Plaintiff Fontenot greatly values his privacy and is very careful with his PII and PHI. Plaintiff stores any documents containing sensitive PII and PHI like his Social Security number in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Moreover, Plaintiff diligently chooses unique usernames and passwords for online accounts storing sensitive PII and PHI. When Plaintiff does entrust a third-party with his PII and PHI, it is only because he understands such information will be reasonably safeguarded

---

[27] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (Feb. 23, 2012), https://web.archive.org/web/20170228020506/http://www.iii.org/insuranceindustryblog/?m=201202 (last visited May 26, 2023).

[28] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), https://web.archive.org/web/20200311212052/http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last visited May 26, 2023).

[29] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://web.archive.org/web/20220131125035if_/https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed May 26, 2023).

from foreseeable threats, and that he will be timely notified if his PII and PHI is exposed.

82. Plaintiff was employed by Defendant from 2004 to 2018 and then again from 2020 to 2022. In the course of his employment relationship with Defendant, Plaintiff provided his PII and PHI, including his full name, date of birth, Social Security number, and phone number, and other sensitive information. Plaintiff reasonably understood that Defendant would encrypt or redact highly sensitive information like his Social Security number, and that such PII and PHI would be deleted after Defendant no longer had a need for it related to his tenure as an employee.

83. As a result of the Data Breach, Plaintiff has spent significant time reviewing his accounts, and reviewing credit reports and financial account statements for indications of actual or attempted identity theft or fraud.

84. Plaintiff has spent significant time, money, and effort on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

85. The Data Breach and exfiltration of Plaintiff's PII has caused him to suffer a loss of privacy. This loss of privacy is analogous to the injury caused by the commission of well-recognized common law privacy torts like invasion of privacy.

86. As a result of the Data Breach, Plaintiff will face a substantial risk of imminent harm for the rest of his life.

87. The fraud, loss of privacy, and substantial risk of harm that Plaintiff faced and continues to face has caused Plaintiff to suffer proportional fear, stress, anxiety, and nuisance.

88. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Defendant was required to adequately protect.

89. Plaintiff has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected, and safeguarded

from future breaches.

CLASS ALLEGATIONS

90. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

91. Plaintiff proposes the following Nationwide Class definition, subject to amendments as appropriate.

> **All persons residing in the United States who were employed by or customers of Defendant whose PII and PHI may have been compromised in the Data Breach.**

92. Excluded from the Classes are the following individuals and/or entities: Acadian Ambulance Service, and Acadian's parents, subsidiaries, affiliates, officers and directors, and any entity in which Acadian has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

93. Plaintiff reserves the right to modify or amend the definition of the proposed classes and any future subclasses before the Court determines whether certification is appropriate.

94. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Classes consist of more than 10,000,000 individuals whose sensitive data was compromised in Data Breach.

95. Commonality. There are questions of law and fact common to the Classes, which

predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII and PHI;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII and PHI;

f. Whether Defendant breached its duty to Class Members to safeguard their PII and PHI;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit

conferred upon them by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

96. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

97. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's Counsel are competent and experienced in litigating class actions.

98. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

99. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for

Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

100. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

101. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

102. The litigation of the claims presented here is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the identifiable Class Members demonstrate that prosecuting this lawsuit as a class action would not present significant manageability problems.

103. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

104. Unless a Class-wide injunction is issued, Defendant may continue in its failure to

properly secure the PII and PHI of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, the PII Defendant continues to maintain will remain at risk of future breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

105. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive relief regarding the Class Members as a whole is appropriate.

106. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security

procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII and PHI; and/or

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and All Class Members)

107. Plaintiff re-alleges and incorporates by reference all the allegations contained in the preceding paragraphs.

108. Plaintiff and Class Members entrusted their PII and PHI to Defendant. Defendant owed to Plaintiff and other Class Members a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the data breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

109. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure to adequately safeguard their PII and PHI in accordance with industry standards concerning data security would result in the compromise of that PII and PHI — just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

110. Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the data breach. This duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the data breach.

111. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable classes of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and Class Members' PII and PHI.

112. The risk that unauthorized persons would attempt to gain access to the PII and PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII and PHI —whether by malware or otherwise.

113. PII and PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and Class Members and the importance of exercising reasonable care in handling it.

114. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiff and Class Members—which actually and proximately caused the Data Breach and injured Plaintiff and Class Members.

115. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary

damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

116. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Invasion of Privacy
(On Behalf of Plaintiff and All Class Members)

117. Plaintiff re-alleges and incorporates by reference all the allegations contained in the preceding paragraphs.

118. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

119. Defendant owed a duty to Plaintiff and Class Members to keep this information confidential.

120. Daixin Team is known to hack VPN to gain initial access to victims' systems. Accordingly, it is more likely than not that one of Defendant's employees recklessly and affirmatively provided Daixin Team with access to Plaintiff's and Class Members' PII and PHI in response to rudimentary phishing communications.

121. The access that Daixin Team was granted to Plaintiff's and Class Members' PII and PHI is highly offensive to a reasonable person.

122. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

123. The data breach constitutes an intentional interference with Plaintiff and Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

124. Defendant acted with a knowing state of mind when it permitted the data breach because it knew its information security practices were inadequate.

125. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

126. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and Class Members to suffer damages.

127. Unless enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause significant and irreparable harm to Plaintiff and Class Members, as their PII and PHI remain under Defendant's care with inadequate cybersecurity systems and policies.

128. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard their PII and PHI.

129. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

130. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

131. Plaintiff re-alleges and incorporates by reference all the allegations contained in the preceding paragraphs.

132. Plaintiff's and Class Members' PII and PHI was provided to Defendant as part of education services or employment that Defendant provided to Plaintiff and Class Members.

133. Plaintiff and Class Members agreed to be employed by Defendant or to pay for Defendant's ambulance services and provided their PII and PHI in the course of that relationship.

134. Defendant and Plaintiff and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiff's and Class Members' PII and PHI, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII and PHI.

135. Defendant had an implied duty of good faith to ensure that the PII and PHI of Plaintiff and Class Members in its possession was only used in accordance with its contractual obligations.

136. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and PHI and to comply with industry standards and applicable laws and regulations for the security of this information.

137. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII and PHI, resulting in the Data Breach.

138. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in the breach of these contracts.

139. As a result of Defendant's conduct, Plaintiff and Class Members did not receive the full benefit of the bargain.

140. Had Defendant disclosed that its data security was inadequate, neither Plaintiff or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

141. As a result of Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII and PHI, as well as the loss of control of their PII and PHI and remain at present risk of suffering additional damages.

142. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all Class Members, request judgment against the Defendant and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiff and his Counsel to

represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant network is compromised, hackers cannot gain access to other portions of Defendant systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how

to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: August 5, 2024

Respectfully Submitted,

By: */s/ Andrew A. Lemmon*
Andrew A. Lemmon (LA Bar No. 18302)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
5301 Canal Boulevard
New Orleans, LA 70124
Tel: (985) 783-6789
alemmon@milberg.com

Bryan L. Bleichner*
Phil J. Krzeski*
CHESTNUT CAMBRONNE
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Attorneys for Plaintiff and the Proposed Class

**Pro hac vice applications forthcoming*

CERTIFICATE OF SERVICE

I certify that on the 2nd day of August 2024, the foregoing document was filed electronically with the Clerk of Court using the Court's CM/ECF system. Notice of this filing will be sent to counsel for all parties by operation of the CM/ECF system.

/s/ Bryan L Bleichner
Bryan L Bleichner*